

24.

- a) Eve will recognize that the plaintext is only one repeated letter because the cipher text is just one repeated letter. Since Eve knows that the key will be something of the form $x \rightarrow x+k$ she will have no way of knowing which letter is repeated in the plaintext, or what the key is.
- b) Eve will recognize that the plaintext is only one repeated letter because the cipher text is just one repeated letter. Eve will have no way of knowing which letter is repeated or what the key is, since no matter what letter is repeated in plaintext there are keys which send every letter to that letter.
- c) The first thing that Eve will notice is that the cipher-text is just the letter 'a' repeated a few hundred times (since the vector (0,0) times $M = (0,0)$ for every 2×2 matrix M). This will automatically tell her that either the block cipher had a poor key, (i.e. $\gcd(\det(M), 26) > 1$) or the plaintext must simply be the letter 'a' repeated. This is true because we know that the equation

$$(x, y) * M = (0, 0)$$

must hold for every consecutive pair of letters in the message, and if the key is not poorly formed ($\gcd(\det(M), 26) = 1$) then the solution to the above equation will be unique. And clearly $x = 0, y = 0$ is a solution to the above equation.